Product Security

- Support for CentOS 7.6 version, on page 1

Support for CentOS 7.6 version

Feature Summary and Revision History

Table 1: Summary Data

Applicable Product(s) or Functional Area	CPS
Applicable Platform(s)	-
Default Setting	Not Applicable
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Table 2: Revision History

Revision Details	Release
CentOS upgraded to 7.6 (1810) Kernel upgraded to 3.10.0-957.10.1.el7	19.3.0
Kernel upgraded to 3.10.0-957.5.1.el7	19.2.0
Kernel upgraded to 3.10.0-957.e17	19.1.0
First introduced: kernel upgraded to 3.10.0-862.14.4.el7.x86_64	18.5.0

Feature Description

CPS now extends support for CentOS version 7.6 (1810) with the kernel upgraded to 3.10.0-957.10.1.el7 version. The CPS packages have been upgraded to be compatible with the updated CentOS version. With this support, CPS is integrated with a more secure and reliable platform.

For service related issues, you can use `journactl` to get systemctl logs.

The following tables list the vulnerabilities that have been fixed as a part of this release:

Table 3: Cisco Internal Alert Manager (CIAM) CVEs

CVE	Name
CVE-2013-4458	GNU glibc getaddrinfo Function Stack Overflow Vulnerability
CVE-2013-1914	GNU glibc getaddrinfo() Function Stack Memory Exhaustion Vulnerability
CVE-2013-4332	GNU glibc Memory Allocation Functions Heap-Based Buffer Overflow Vulnerability
CVE-2013-0242	GNU glibc Regular Expression Matching Routines Denial of Service Vulnerability
CVE-2013-4237	GNU glibc readdir_r() Function Buffer Overflow Vulnerability
CVE-2018-1088	Glusterfs Snapshot Scheduler Privilege Escalation Vulnerability
CVE-2018-5407	Computing Processor PortSmash Side-Channel Information Disclosure Vulnerability
CVE-2018-1086	ClusterLabs pcs Debug Parameter Removal Bypass Information Disclosure Vulnerability
CVE-2018-10852	SSSD UNIX Pipe Information Disclosure Vulnerability
CVE-2018-18559	Linux Kernel Use-After-Free Race Condition Vulnerability
CVE-2018-18397	Linux Kernel userfaultfd Implementation Unauthorized Access Vulnerability
CVE-2018-14646	Linux Kernel __netlink_ns_capable() Function NULL Pointer Dereference Denial of Service Vulnerability
CVE-2018-17972	Linux Kernel proc_pid_stack() Function Kernel Task Stack Contents Disclosure Vulnerability
CVE-2018-14633	Linux Kernel chap_server_compute_md5() Stack Buffer Overflow Denial of Service Vulnerability

Table 4: Nessus CVEs

CVE	Name
CVE-2019-6454	CentOS 7 : systemd (CESA-2019:0368)
CVE-2018-9568	CentOS 7 : kernel (CESA-2019:0512)
CVE-2018-18445	CentOS 7 : kernel (CESA-2019:0512)
CVE-2018-17972	CentOS 7 : kernel (CESA-2019:0512)

Table 5: CentOS 7 CVEs

CVE	Name
CVE-2004-2761	CentOS 7 : polkit (CESA-2019:0230)
CVE-2018-5407	CentOS 7 : openssl (CESA-2019:0483)